JOURNAL OF ALGEBRA 32, 576–599 (1974)

An Invariant Ideal of a Group Ring of a Finite Group, and Applications

J. S. HSIA AND ROGER D. PETERSON*

Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, Ohio 43210

Communicated by A. Fröhlich

Received July 26, 1973

0. INTRODUCTION

Let R be a ring with identity and G a finite group and RG the group ring. The *invariant ideal* of R is $\gamma_R(G) = R \cap \Gamma_R(G)$, where $\Gamma_R(G)$ is the right ideal of RG generated by elements of the form $\sigma(H) = \sum_{h \in H} h$, $1 \neq H$ a subgroup of G. If R is the ring of rational integers, set $\gamma_{\mathbf{Z}}(G) = \nu(G)\mathbf{Z}$ and we call $\nu(G)$ the *numerical invariant* of the finite group G. This latter (non-negative) invariant was originally introduced in [3] to study the behavior of the Witt group of quadratic forms under finite Galois field extensions with Galois group G. In particular, therefore, it was useful in obtaining informations on various arithmetical invariants of fields arising from quadratic form theory. For an elementary abelian group of order p^n with $n > 1$, $\nu(G)$ was calculated in [3] to have the value p, and it was also remarked in that paper that the general determination for the numerical invariant would involve complicated group-theoretical questions. This is indeed the case. In this paper we extend the study of $\nu(G)$ to the invariant ideal $\gamma_R(G)$, where R is any ring with identity. We present several general results on this invariant, among which the useful "reduction theorems" in Section 1.D are most fundamental. We also exhibit explicit numerical results of the invariant for several large classes of groups (e.g., general and special linear groups, simple groups, and most solvable groups). The short Section 2 deals with some applications of the numerical invariant.

In Section 1.A we present some preliminary results on the invariant ideal. The main result (Theorem 1.A.4) is that the invariant ideal is trivial if the group has precisely one subgroup of prime order for each prime dividing its order. Section 1.B shows that for a p-group the invariant ideal is always the principal ideal pR unless the group is either cyclic or generalized quaternion.

* Current address: Department of Mathematics, University of Wisconsin, Milwaukee, Wisconsin 53201.

Section 1.C introduces the notion of a *tight group* which is, in essence (certainly in the solvable case), the basic building block that determines the invariant ideal. As groups tend to possess tight subgroups, its determination is vital and this is presented in Theorem 1.C.2. From this, as well as the use of several "sledge-hammer" results from group theory, it is shown that $\gamma_R(G) = R$ for all finite nonabelian simple groups G (Corollary 1.C.3). The three reduction theorems in Section 1.D are fundamental as they are used throughout. Of the three, the third (Theorem 1.D.4) is the most significant. Together they enable us to "descend" from the full group to certain of its subgroups. Sections 1.E and 1.F devote to extracting some consequences of the reduction theorems (see, for instance, Theorem 1.E.1, Corollary 1.E.2, Theorem 1.F.2, and Corollaries 1.F.4 and 1.F.5). Also, Corollary 1.F.3 generalizes (and completes) Lemma 4 of [7] to all solvable groups. This Section 1.F also serves to illustrate the sharp distinction and complication of the invariant ideal between the solvable and the nonsolvable cases. Namely, in the solvable case, the numerical invariant of G is completely determined by the numerical invariants of the tight subgroups of G. In particular, $\nu(G) = 0$ if and only if G has no tight subgroups. Using a theorem of Suzuki (see Appendix) one can determine all finite nonsolvable groups all of whose Sylow subgroups have vanishing numerical invariant. Also, for an odd prime p, $SL(2, p^n)$ has no tight subgroups if and only if $n = 1$ and p is a Fermat prime. On the other hand, for p a Fermat prime greater than 5, $\nu(SL(2, p))$ is divisible by p (see Proposition 1.G.4 and Appendix), and is not zero! Section 1.G computes the explicit values of the numerical invariant for general and special linear groups.

Some applications of the numerical invariant are cited in three short sections. We show how a privately communicated theorem of Pfister on the height of a field together with the knowledge of the numerical invariant can sharply improve known estimates of the height behavior under Galois field extensions. Also, some estimates are given or mentioned about the generalized Kaplansky's u-invariant as well as for the number of square classes and for the size of the Witt ring under finite field extensions. The same technique is then used to derive estimates in class number behaviour under finite field extensions. Finally, a result of Scharlau's linking the fixed-point-free representations of a finite group with the vanishing of the numerical invariant of the group is cited, and in the solvable case such groups are characterized (see Appendix).

1.

A. *Definition of the Invariant and Preliminary Results*

Throughout this Section 1, unless otherwise mentioned, R is an associative ring with identity and G is a finite group. Let RG be the group ring for G over

R, and $\Gamma_R(G)$ be the right ideal of RG generated by the set $\{\sigma(H) = \sigma_R(H) = \sum_{h\in H} h \mid 1 \neq H$ a subgroup of $G\}$. Let $\gamma_R(G) = R \cap \Gamma_R(G)$. Of course, $\Gamma_R(1) = 0$, so that $\gamma_R(1) = 0$. If H is a nontrivial subgroup of G, and $g \in G$, $r \in R$, we have $g\sigma(H) = \sigma(gHg^{-1})g$ and $r\sigma(H) = \sigma(H)r$. Hence, $\Gamma_R(G)$ is also the left (and so two-sided) ideal generated by the $\sigma(H)$'s. Suppose H and K are subgroups of G, and $H \leqslant K$, and $\{x_1, ..., x_n\}$ is a full representative set for the right cosets of H in K, then

$$\sigma(K) = \sum_{k\in K} k = \sum_i \Big(\sum_{g\in Hx_i} g \Big) = \Big(\sum_{h\in H} h \Big) \Big(\sum_i x_i \Big) = \sigma(H)x.$$

Taking left cosets of H in K and repeating the calculation, we see $\sigma(K) = y\sigma(H)$ for some $y \in RG$. Thus, we have the following:

1.A.1. *$\Gamma_R(G)$ is the right ideal (and also the left ideal) of RG generated by the set $\{\sigma(H) \mid H$ is a subgroup of prime order in $G\}$.*

1.A.2. *If $G = HK$ with $H \cap K = 1$, then $\sigma(G) = \sigma(H)\,\sigma(K)$.*

Clearly, if H is a subgroup of G, then $\gamma_R(H) \subseteq \gamma_R(G)$. The following rules are also useful and we record them here.

1.A.3. *For each subgroup H of G, we have*: (i) $h\sigma(H) = \sigma(H)h = \sigma(H)$, $h \in H$; (ii) $(1 - h)\,\sigma(H) = \sigma(H)(1 - h) = 0$; (iii) $\sigma(H)^2 = |H|\,\sigma(H)$; (iv) $RG\sigma(G) = \sigma(G)\,RG = R\sigma(G)$.

The next result, though simple in proof, is very useful.

THEOREM 1.A.4. *If G has exactly one subgroup of prime order for each prime dividing the order $|G|$ of G (e.g., when G is cyclic or generalized quaternion), then $\gamma_R(G) = 0$.*

Proof. Let $H_1 = \langle h_1\rangle, ..., H_n = \langle h_n\rangle$ be the n distinct prime order subgroups of G. Then, all the H_i's are normal in G, and $\langle h_1, ..., h_n\rangle = H_1 \times \cdots \times H_n$. Let $\alpha = (1 - h_1) \cdots (1 - h_n)$. Since $(1 - h_i)\,\sigma(H_i) = 0$ and $(1 - h_i)(1 - h_j) = (1 - h_j)(1 - h_i)$ for all i, j, we have $\alpha\sigma(H_i) = 0$ for all i. By 1.A.1, $\Gamma_R(G) = \sum_i \sigma(H_i)\,RG$. Thus, α annihilates $\Gamma_R(G)$ and so also $\gamma_R(G)$. But the coefficient $\text{coeff}_\alpha(1)$ of α at 1 equals 1. We are done.

EXAMPLE. $G = Q \times C$, where Q is generalized quaternion and C cyclic with odd order. $G = \langle a, b \mid a^4 = b^3 = 1,\ a^{-1}ba = b^{-1}\rangle$. In the second example one notes that G modulo the center is isomorphic to S_3, which will be shown in Section 1.C to have $\gamma_R(S_3) = 3R$.

B. *Groups of Prime Power Order.*

1.B.1. *If G is a p-group, p a prime, then $\gamma_R(G) \subseteq pR$.*

Proof. Define the ring epimorphism $\phi: RG \to R/pR$ by the rule $\sum_{g\in G} r_g g \mapsto (\sum_{g\in G} r_g) + pR$. If H is a nontrivial subgroup, $\phi(\sigma(H)) = 0 + pR$, so that $\gamma_R(G) = R \cap \Gamma_R(G) \subseteq R \cap \mathrm{Ker}(\phi) = pR$.

1.B.2. *If G is a p-group for some prime p, then $\gamma_R(G) = 0$ if G is either cyclic or generalized quaternion, and $=pR$ if otherwise.*

Proof. If G is cyclic or generalized quaternion, we have Theorem 1.A.4. Otherwise, G has an elementary abelian subgroup of order p^2. A calculation as in Section 4 of [6] shows $p \in \gamma_R(G)$. 1.B.1 now finishes the argument.

COROLLARY 1.B.3. *If G is a p-group and R has characteristic p, then $\gamma_R(G) = 0$. If P and Q are Sylow subgroups of G such that $|P| \neq |Q|$, $\gamma_{\mathbf{Z}}(P) \neq 0$ and $\gamma_{\mathbf{Z}}(Q) \neq 0$, then $\gamma_R(G) = R$.*

C. *Tight Groups.*

Let p and q be primes. There is at most one nonabelian group of order pq. Such a group exists if and only if either $p \mid q - 1$ or $q \mid p - 1$.

DEFINITION 1.C.1. Let H be a group. We say H is *tight* if and only if H is a noncyclic group of order pq, where p and q are (not necessarily distinct) primes.

Groups tend to have tight subgroups so that the calculation of the invariant for tight groups is important.

THEOREM 1.C.2. *If G is a nonabelian tight group of order pq with $p < q$, then $\gamma_R(G) = qR$.*

Proof. Write $G = \langle a, b \mid a^p = b^q = 1, a^{-1}ba = b^r\rangle$, where $r \in \mathbf{Z}$, $r^p \equiv 1 \pmod q$ and $r \not\equiv 1 \pmod q$. Let $P = \langle a\rangle$ and $Q = \langle b\rangle$. Then $G = PQ$, $Q \lhd G$, $P \cap Q = 1$. We have $(ab^i)^j = a^j b^{i(1-r^j)/(1-r)}$ for all i, j. In particular, ab^i has order p. We have the following:

$$\sum_{i=0}^{q-1} \sigma(\langle ab^i\rangle) = \sum_{i=0}^{q-1}\sum_{j=0}^{p-1} (ab^i)^j = \sum_{i=0}^{q-1}\sum_{j=0}^{p-1} a^j b^{i(1-r^j)/(1-r)}$$

$$= \sum_{j=0}^{p-1} a^j \left(\sum_{i=0}^{q-1} \left(b^{(1-r^j)/(1-r)}\right)^i\right) = q + \sum_{j=1}^{p-1} a^j \left(\sum_{i=0}^{q-1} \left(b^{(1-r^j)/(1-r)}\right)^i\right)$$

$$= q + \sum_{j=1}^{p-1} a^j \sigma(\langle b\rangle) = q + (\sigma(P) - 1)\,\sigma(Q)$$

$$= q + \sigma(G) - \sigma(Q).$$

Therefore, $q \in \gamma_R(G)$. To show $\gamma_R(G) \subseteq qR$, let $P_1, \ldots, P_n$ be the subgroups of G with order p. Then, 1.A.1 tells us

$$\Gamma_R(G) = RG\sigma(Q) + \sum_{i=1}^{n} RG\sigma(P_i).$$

Suppose $r \in \gamma_R(G)$. Write $r = a_0\sigma(Q) + \sum_{i=1}^{n} a_i\sigma(P_i)$ with $a_0, \ldots, a_n$ in RG. Then,

$$r\sigma(Q) = a_0\sigma(Q)^2 + \sum_{i=1}^{n} a_i\sigma(P_i)\,\sigma(Q) = a_0q\sigma(Q) + \sum_{i=1}^{n} a_i\sigma(G).$$

Hence, $r\sigma(Q)$ belongs to $qRG + RG\sigma(G) = qRG + R\sigma(G)$. But if $r\sigma(Q) = qa + x\sigma(G)$ with $a \in RG$ and $x \in R$, then a comparison of the coefficients shows that $r \in qR$. The proof is completed.

COROLLARY 1.C.3. *If G is a nonabelian finite simple group, then $\gamma_R(G) = R$.*

Proof. The proof given here employs several "sledge-hammer" theorems from group theory. By Feit–Thompson, G must have even order. If a Sylow 2-subgroup is cyclic, then a standard application of Burnside's normal p-complement theorem (see [1, p. 252]) leads to a contradiction. A theorem of Brauer–Suzuki (see [1, p. 373]) shows that a Sylow 2-subgroup cannot be generalized quaternion. Therefore, G contains a tight subgroup T of order 4. Next, a theorem of Suzuki (see [9]) says G has two elements a, b each of order two (involutions) and such that the subgroup $\langle a, b\rangle$ they generate is not a 2-group. This means then G must have also a dihedral subgroup D of order $2p$ for some *odd* prime p. But, $\gamma_R(T) = 2R$ and $\gamma_R(D) = pR$ by 1.B.2 and Theorem 1.C.2, respectibely. Hence $\gamma_R(G) = R$.

At this point, let us define the *numerical invariant* $\nu(G)$ of a finite group G to be that nonnegative rational integer given by $\nu(G)\mathbf{Z} = \gamma_{\mathbf{Z}}(G)$. Thus, if G has at least one tight subgroup, then $\nu(G) = 1$ or p for some prime p dividing $|\,G\,|$.

1.C.4. $\nu(G)\,R \subseteq \gamma_R(G)$.

Proof. There is a unique ring homomorphism $\phi\colon \mathbf{Z}G \to RG$ with $\phi(g) = g$, $g \in G$. We have $\phi(\sigma_{\mathbf{Z}}(H)) = \sigma_R(H)$ for every subgroup H of G. So, $\nu(G)R \subseteq R \cap \Gamma_R(G) = \gamma_R(G)$.

EXAMPLES 1.C.5. (Symmetric and Alternating Groups.) Clearly, $\nu(S_1) = \nu(S_2) = \nu(A_2) = 0$. Since S_3 is a nonabelian tight group, $\nu(S_3) = 3$. A_3, being cyclic, has $\nu(A_3) = 0$. Since S_4 contains S_3 as well as an elementary abelian group of order 4, $\nu(S_4) = 1$. It can be shown that $\nu(A_4) = 2$ (see Section 1.E). From the simplicity of A_n for $n \geqslant 5$, we have $\nu(A_n) = \nu(S_n) = 1$.

D. *Reduction Theorems.*

From the last section we know that if G has tight subgroups H and K such that their invariant ideals $\gamma_R(H), \gamma_R(K)$ are different, then $\gamma_R(G)$ must be R. The question then arises as to what happens if G has either no tight subgroups at all, or when it does have them they all give rise to the same invariant ideal. Therefore, it is essential that we need some "descent" theorems in order to help characterize the invariant ideal in terms of the subgroups of G. The three reduction theorems presented here are extremely useful. Their applications will be investigated in Section 1.E.

Let $H_1 = \langle h_1 \rangle, \ldots, H_n = \langle h_n \rangle$ be the full list of prime-order subgroups of G, and $| H_i | = p_i$. Then, $\Gamma_R(G) = \sum_i RG\sigma(H_i)$. Suppose $y \in \Gamma_R(G)$, write $y = \sum_i a_i\sigma(H_i)$, $a_i \in RG$. Then, there exists a subset $\{\theta_g^{(i)} \mid g \in G,\ 1 \leqslant i \leqslant n\}$ of R such that $a_i = \sum_{g \in G} \theta_g^{(i)} g$. We have then

$$y = \sum_i \sum_{g \in G} \theta_g^{(i)} g\sigma(H_i) = \sum_i \sum_{g \in G} \sum_{j=0}^{p_i - 1} \theta_g^{(i)} g h_i^{\,j} = \sum_{g \in G} \left(\sum_i \sum_j \theta_{gh_i^{-j}}^{(i)} \right) g.$$

Comparing coefficients, we see $\operatorname{coeff}_y(g) = \sum_{i=1}^{n} \sum_{j=0}^{p_i - 1} \theta_{gh_i^{-j}}^{(i)}$ for all $g \in G$. This proves the following:

PROPOSITION 1.D.1. *Suppose $H_1, \ldots, H_n$ is the full list of prime-order subgroups of G with $H_i = \langle h_i \rangle$ and $| H_i | = p_i$. Let $y \in RG$. Then, $y \in \Gamma_R(G) \Leftrightarrow$ there is a finite subset $\{\theta_g^{(i)} \mid g \in G,\ 1 \leqslant i \leqslant n\}$ of R such that $\operatorname{coeff}_y(g) = \sum_{i=1}^{n} \sum_{j=0}^{p_i - 1} \theta_{gh_i^{-j}}^{(i)}$ for all $g \in G$. In particular, if $y \in R$, then $y \in \gamma_R(G) \Leftrightarrow$ the above finite subset of R satisfies*

$$\sum_{i=1}^{n} \sum_{j=0}^{p_i - 1} \theta_{gh_i^{-j}}^{(i)} = \begin{cases} y & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} \quad \text{for all } g \in G.$$

From this technical and computational result we immediately get our first reduction theorem; namely:

THEOREM 1.D.2. *Suppose H is a subgroup of G and H contains every prime-order subgroup of G. Then $\gamma_R(G) = \gamma_R(H)$.*

Remark. If we just wanted Theorem 1.D.2, we could obtain it by a direct coset calculation. However, Proposition 1.D.1 will be used very often in later sections.

THEOREM 1.D.3. *Let $G = P \times N$ where P is a cyclic p-group for some prime p, and $p \nmid | N |$. Then $\gamma_R(G) = \gamma_R(N)$.*

Proof. If P_0 is the prime-order subgroup of P, then $G_0 = P_0 \times N$ contains every prime-order subgroup of G so that by Theorem 1.D.2,

$\gamma_R(G) = \gamma_R(G_0)$. Hence, we may assume $|P| = p$ already. Let $P = \langle a \rangle$, $\alpha = \sigma(P)$, and $H_1, \ldots, H_n$ be the full list of prime-order subgroups of N where $H_i = \langle h_i \rangle$ has order p_i. Set $\beta_i = \sigma(H_i)$. We have then

$$\Gamma_R(G) = RG\alpha + \sum_i RG\beta_i .$$

Suppose $r \in \gamma_R(G)$. Then, 1.D.1 says there exist subsets $\{\theta(t, y) \mid t \in P, y \in N\}$ and $\{\pi^{(i)}(t, y) \mid t \in P, y \in N, 1 \leqslant i \leqslant n\}$ of R such that

$$r = \Big(\sum_{t\in P}\sum_{y\in N} \theta(t, y)\, ty\Big)\,\alpha + \sum_{i=1}^{n} \Big(\sum_{t\in P}\sum_{y\in N} \pi^{(i)}(t, y)\, ty\Big)\,\beta_i .$$

We have

$$r = \sum_{t\in P}\sum_{y\in N}\sum_{j=0}^{p-1} \theta(t, y)\, tya^j + \sum_{i=1}^{n}\sum_{t\in P}\sum_{y\in N}\sum_{j=0}^{p_i-1} \pi^{(i)}(t, y)\, h_i^j$$

$$= \sum_{t\in P}\sum_{y\in N}\sum_{j=0}^{p-1} \theta(t, y)(ta^j)y + \sum_{i=1}^{n}\sum_{t\in P}\sum_{y\in N}\sum_{j=0}^{p_i-1} \pi^{(i)}(t, y)\, t(yh_i^j).$$

Computing the coefficients, we get:

$$\operatorname{coeff}_r(ty) = \sum_{j=0}^{p-1} \theta(ta^{-j}, y) + \sum_{i=1}^{n}\sum_{j=0}^{p_i-1} \pi^{(i)}(t, yh_i^{-j})$$

$$= \sum_{x\in P} \theta(x, y) + \sum_{i=1}^{n}\sum_{j=0}^{p_i-1} \pi^{(i)}(t, yh_i^{-j}).$$

Note that the first term on the right side does not depend on t. Since $\operatorname{coeff}_r(ay) = 0$ for all $y \in N$, we get

$$\sum_{x\in P} \theta(x, y) = -\sum_{i=1}^{n}\sum_{j=0}^{p_i-1} \pi^{(i)}(a, yh_i^{-j}) \qquad \text{for all} \quad y \in N.$$

Therefore,

$$\operatorname{coeff}_r(ty) = \sum_{i=1}^{n}\sum_{j=0}^{p_i-1} \pi^{(i)}(t, yh_i^{-j}) - \pi^{(i)}(a, yh_i^{-j}).$$

Letting $\Delta_y^{(i)} = \pi^{(i)}(1, y) - \pi^{(i)}(a, y)$, we have $\{\Delta_y^{(i)} \mid y \in N, 1 \leqslant i \leqslant n\} \subseteq R$, and

$$\sum_{i=1}^{n}\sum_{j=0}^{p_i-1} \Delta_{yh_i^{-j}}^{(i)} = \operatorname{coeff}_r(y) = \begin{cases} r & \text{if } y = 1 \\ 0 & \text{if } y \neq 1. \end{cases}$$

Hence, $r \in \gamma_R(N)$ by Proposition 1.D.1, and we have: $\gamma_R(G) \subseteq \gamma_R(N) \subseteq \gamma_R(G)$.

While we are engrossed with these technical intricacies, we present our third and last reduction theorem whose proof is equally computational and yet sufficiently different to warrant the details to be included. It also is the strongest of the three reduction steps.

THEOREM 1.D.4. *Suppose $G = HQ$, where Q is a Sylow q-subgroup of G for some prime q, $Q \lhd G$, and $q \nmid |H|$. Then, we have:*

$$\gamma_R(G) \subseteq R \cap (\Gamma_R(H) + q \cdot RH).$$

Proof. Let $H_1, \ldots, H_n$ be the prime-order subgroups of H with $H_i = \langle h_i \rangle$, $|H_i| = p_i$, and $\alpha_i = \sigma(H_i)$. Let $Q_1, \ldots, Q_m$ be the order-q subgroups of Q with $Q_i = \langle a_i \rangle$ and $\beta_i = \sigma(Q_i)$. Then the set of prime-order subgroups of G is $\{Q_1, \ldots, Q_m\} \cup \{x^{-1}H_i x \mid x \in Q, 1 \leqslant i \leqslant n\}$. And,

$$\Gamma_R(G) = \sum_i RG\beta_i + \sum_{x \in Q} \sum_i RG\alpha_i x.$$

Suppose $r \in \gamma_R(G)$, then there exist subsets $\{\theta_i(t, y) \mid 1 \leqslant i \leqslant m, t \in H, y \in Q\}$ and $\{\pi_i^{(x)}(t, y) \mid 1 \leqslant i \leqslant n, t \in H, \text{ and } x, y \in Q\}$ of R such that

$$r = \sum_{i=1}^{m} \left(\sum_{t \in H} \sum_{y \in Q} \theta_i(t, y)\, ty \right) \beta_i + \sum_{x \in Q} \sum_{j=1}^{n} \left(\sum_{t \in H} \sum_{y \in Q} \pi_i^{(x)}(t, y)\, ty \right) \alpha_j x.$$

We have

$$r = \sum_{i=1}^{m} \sum_{t \in H} \sum_{y \in Q} \sum_{k=0}^{q-1} \theta_i(t, y)\, tya_i^k + \sum_{x \in Q} \sum_{j=1}^{n} \sum_{t \in H} \sum_{y \in Q} \sum_{k=0}^{p_i - 1} \pi_i^{(x)}(t, y)\, tyh_i^k x.$$

Computing the coefficients, we get

$$\operatorname{coeff}_r(t_0 y_0) = \sum_{j=1}^{m} \sum_{w=0}^{q-1} \theta_j(t_0, y_0 a_j^{-w}) + \sum_{i=1}^{n} \sum_{k=0}^{p_i - 1} \sum_{x \in Q} \pi_i^{(x)}(t_0 h_i^{-k}, h_i^k y_0 x^{-1} h_i^{-k})$$

for all $t_0 \in H, y_0 \in Q$.

This gives

$$\begin{aligned} \operatorname{coeff}_r(t_0) &= \sum_{y_0 \in Q} \operatorname{coeff}_r(t_0 y_0) \\ &= \sum_{y_0 \in Q} \sum_{j=1}^{m} \sum_{w=0}^{q-1} \theta_j(t_0, y_0 a_j^{-w}) \\ &\quad + \sum_{y_0 \in Q} \sum_{i=1}^{n} \sum_{k=0}^{p_i - 1} \sum_{x \in Q} \pi_i^{(x)}(t_0 h_i^{-k}, h_i^k y_0 x^{-1} h_i^{-k}) \end{aligned}$$

for all $t_0 \in H$.

There is a collapsing of terms in the second variable of the coefficients. (Namely, as y_0 runs through Q, the term $\theta_j(t_0, y_0 a_j^{-w})$ runs through all terms of the form $\theta_j(t_0, y_0)$ and likewise, the term $\pi_i^{(x)}(t_0 h_i^{-k}, h_i^k y_0 x^{-1} h_i^{-k})$ runs through all terms of the form $\pi_i^{(x)}(t_0 h_i^{-k}, y_0)$.) Therefore, the equation simplifies to

$$\operatorname{coeff}_r(t_0) = \sum_{y_0 \in Q} \sum_{j=1}^{m} \sum_{w=0}^{q-1} \theta_j(t_0, y_0) + \sum_{y_0 \in Q} \sum_{i=1}^{n} \sum_{k=0}^{p_i-1} \sum_{x \in Q} \pi_i^{(x)}(t_0 h_i^{-k}, y_0).$$

We notice that the index w does not appear in the summand for the first term. Hence, for all $t_0 \in H$,

$$\operatorname{coeff}_r(t_0) = q \cdot \sum_{y_0 \in Q} \sum_{j=1}^{m} \theta_j(t_0, y_0) + \sum_{y_0 \in Q} \sum_{i=1}^{n} \sum_{k=0}^{p_i-1} \sum_{x \in Q} \pi_i^{(x)}(t_0 h_i^{-k}, y_0).$$

Letting $\theta_{t_0} = \sum_{j=1}^{m} \sum_{y_0 \in Q} \theta_j(t_0, y_0)$ and $\pi_0^{(i)} = \sum_{x \in Q} \sum_{y_0 \in Q} \pi_i^{(x)}(t_0, y_0)$. We have then $r = \sum_{i=1}^{n} (\sum_{t_0 \in H} \pi_{t_0}^{(i)} t_0)\, \alpha_i + q \cdot (\sum_{t_0 \in H} \theta_{t_0} t_0)$, so that indeed r belongs to $\Gamma_R(H) + q \cdot RH$, finishing the proof.

Remark. If G has a tight subgroup T with $\nu(T) = q$ in the above theorem, then $\gamma_R(G) = R \cap (\Gamma_R(H) + q \cdot RH)$. Theorem 1.D.4, together with the Schur–Zassenhaus Theorem (see [1, p. 221]), says that if G has a normal Sylow q-subgroup Q for some prime q, then $\gamma_R(G)$ is contained in $R \cap (\Gamma_R(H) + q \cdot RH)$ where H is the subgroup $\cong G/Q$. Loosely speaking then, if S is a normal Sylow subgroup of G, then $\gamma_R(G)$ is more-or-less determined by the tight subgroups of G and $\gamma_R(G/S)$. This provides us with an induction step.

E. *Some Consequences of the Reduction Theorems*

In this section we use the reduction theorems to extract some concrete answers on the numerical invariant for some classes of solvable groups. A group G is said to satisfy *condition* $(*)$ if it has exactly one subgroup of prime-order for each prime dividing $|G|$.

THEOREM 1.E.1. *Let G be a nilpotent group. Then, we have the following*: (1) $\gamma_R(G) = \nu(G)R$. (2) $\nu(G) = \text{g.c.d.}(\{\nu(S) \mid S \text{ is a Sylow subgroup of } G\})$. (3) $\nu(G) = \text{g.c.d.}(\{\nu(T) \mid T \text{ is a tight subgroup of } G\})$. (4) $\nu(G) = 0, 1,$ *or* p *for some prime dividing* $|G|$. (5) $\nu(G) = 0 \Leftrightarrow G$ *satisfies condition* $(*)$. (6) $\nu(G) = p \Leftrightarrow G = P \times N$, *where P is a Sylow p-subgroup of G, $\nu(P) = p$, and N has exactly one subgroup of prime order for each prime dividing* $|G|$. (7) $\nu(G) = 1 \Leftrightarrow G$ *has an abelian subgroup of type* (p, p, q, q), *where p and q are distinct primes.*

We shall only mention here that in the case when there is only one Sylow

subgroup with nonvanishing numerical invariant, successive applications of Theorem 1.D.3 give the desired answer. The other cases are easy to handle.

COROLLARY 1.E.2. *If G is abelian, then $\nu(G) = 0$ if and only if G is cyclic.*

PROPOSITION 1.E.3. *Suppose Q is a Sylow q-subgroup of G, $Q \lhd G$, and G/Q satisfies condition $(*)$. Then we have the following*: (1) $\gamma_R(G) = \nu(G)R$. (2) $\nu(G) = 0$ *or* q. (3) $\nu(G) = \text{g.c.d.}(\{\nu(T) \mid T \text{ is a tight subgroup of } G\})$.

Proof. By Schur–Zassenhaus, we may write $G = HQ$, where $q \nmid |H|$ and H satisfies *condition* $(*)$. Let A be the subgroup of H generated by the prime-order subgroups of H, then A is cyclic and the subgroup AQ contains every prime-order subgroup of G, so that by Theorem 1.D.2 $\gamma_R(G) = \gamma_R(AQ)$. By Theorem 1.D.4, $\gamma_R(AQ)$ is contained in $R \cap (\Gamma_R(A) + q \cdot RA)$. Suppose $r \in R \cap (\Gamma_R(A) + q \cdot RA)$. Write $r = a + qb$, $a \in \gamma_R(A)$ and $b \in RA$. From the proof of Theorem 1.4.A, there exists $c \in RA$ such that $\text{coeff}_c(1) = 1$ and $\Gamma_R(A)c = 0$. So, $rc = qbc$ and $r = \text{coeff}_{rc}(1) = \text{coeff}_{qbc}(1) \in qR$. Thus, we have: $\gamma_R(G) \subseteq q \cdot R$. Also, in the remainder of this proof we may assume G/Q is cyclic. We treat in cases.

Case 1. $\nu(Q) \neq 0$. Then, $q = \nu(Q) \in \gamma_R(G) \subseteq qR$, so that $\gamma_R(G) = qR = \nu(G)R$ and $\nu(G) = q$. (3) is clearly true.

Case 2. Q is cyclic. Consider the centralizer $C_G(Q)$, which is clearly cyclic. Either $C_G(Q)$ contains every prime-order subgroup of G or there is a subgroup P of G of prime order p such that PQ contains a nonabelian group of order pq. In the former case, $\gamma_R(G) = \gamma_R(C_G(Q)) = 0$ and G has no tight subgroups. In the latter case, we have $q = \nu(PQ)$ and $\gamma_R(G) = qR$, $\nu(G) = q$.

Case 3. Q is generalized quaternion. Suppose $G/C_G(Q)$ is a 2-group. Then $C_G(Q)$ contains every prime-order subgroup of G, and is also cyclic. In this case, G has no tight subgroups and $\gamma_R(G) = \gamma_R(C_G(Q)) = 0$. So, assume $G/C_G(Q)$ is *not* a 2-group. Since $G/C_G(Q) = N_G(Q)/C_G(Q)$ is isomorphic to a subgroup of the automorphism group of Q, and since Q is generalized quaternion, the index $[G: C_G(Q)]$ divides 24, $|Q| = 8$, and $3 \mid [G: C_G(Q)]$. In particular, 3 must divide $|G|$. Since a Sylow 3-subgroup of G is cyclic, and since $C_G(Q)$ does not contain every prime-order subgroup of G, it follows that $9 \nmid |G|$. Therefore, we must have: $|G| = 24m$ with $m \geqslant 1$, and $6 \nmid m$.

Let H be a subgroup of G with $|H| = m$ (Hall Theorem). Thus, H (being isomorphic to a subgroup of G/Q) is cyclic. Also, $3 \mid |C_G(H)|$ as H lies in a cyclic subgroup of order $3m$. Consider HQ. If L is a subgroup of Q, then $N_{HQ}(L)/C_{HQ}(L)$ is a 2-group. By Frobenius normal p-complement theorem (see [1, p. 253]), $H \lhd HQ$, so that $HQ = H \times Q$. Hence, $|C_G(H)| = 24m$

and so H is contained in the center of G. This yields $G = S \times H$ where $|S| = 24$, Q is a Sylow 2-subgroup of S, and $3 \mid [S: C_S(Q)]$. Therefore, $S \cong SL(2, 3)$, and $G \cong SL(2, 3) \times H$, where H is cyclic, and $6 \nmid |H|$. Applying Theorem 1.D.3 successively, we deduce that $\nu(G) = \nu(SL(2, 3))$ and $\gamma_R(G) = \gamma_R(SL(2, 3))$. Also, G has no tight subgroups. But, $\gamma_R(SL(2, 3)) = 0$!! (See Appendix.) We are finished.

COROLLARY 1.E.4. *Suppose* $|G| = pq^n$, *where* $n \geqslant 1$ *and* p, q *are primes with* $p < q$. *Then* $\gamma_R(G)$ *is* 0 *if* G *is cyclic, and is* qR *if otherwise.*

COROLLARY 1.E.5. *Let* G *be the dihedral group of order* $2n$ *where* $n \geqslant 3$. *Then* $\gamma_R(G)$ *is* pR *if* n *is a* p*-power for some prime* p, *and is* R *if otherwise.*

COROLLARY 1.E.6. *Let* G *be a* p, q*-group (i.e.,* $|G| = p^s q^t$*), where* p *and* q *are primes with* $p < q$. *Assume* G *has a normal Sylow* q*-subgroup. Then we have*: (1) $\gamma_R(G) = \nu(G)R$. (2) $\nu(G) = 0$, 1, p, *or* q. (3) $\nu(G) = 0 \Leftrightarrow G$ *has at most one subgroup of order* p *and at most one subgroup of order* q. (4) $\nu(G) = p \Leftrightarrow G$ *has an elementary abelian subgroup of order* p^2, G *has no nonabelian tight subgroup, and the Sylow* q*-subgroup is cyclic.* (5) $\nu(G) = q \Leftrightarrow$ *a Sylow* p*-subgroup is cyclic or generalized quaternion, and* G *has a tight subgroup with* $\nu = q$. (6) $\nu(G) = 1 \Leftrightarrow G$ *has tight subgroups with different* ν*-values.* (7) $\nu(G) =$ g.c.d.$(\{\nu(T) \mid T$ *a tight subgroup of* $G\}$.)

F. *Solvable Groups Having* $\nu = 0$ *for all Sylow Subgroups*

This section aims at describing the invariant ideal $\gamma_R(G)$ when the group G is a solvable group all of whose Sylow subgroups have their numerical invariant vanishing. Thus, the odd-order Sylow subgroups of G must all be cyclic and a Sylow 2-subgroup must be either cyclic or generalized quaternion. It is well-known that if p is the least prime dividing $|G|$, and a Sylow p-subgroup of G is cyclic, then G has a normal p-complement. Using this, one can deduce: if every Sylow subgroup of G is cyclic, and q is the largest prime dividing $|G|$, then G has a normal Sylow q-subgroup (so that, in particular, G is solvable). More generally, we have the following:

LEMMA 1.F.1. *Let* G *be solvable and* $\nu(S) = 0$ *for every Sylow subgroup* S *of* G, *and if* $q > 3$ *is the largest prime divisor of* $|G|$, *then* G *has a normal Sylow* q*-subgroup.*

Proof. We may suppose the Sylow 2-subgroup is generalized quaternion. A Sylow 2-subgroup Q of G lies in a Hall $2'$-subgroup H of G. Hence, $Q \lhd H$, and $[G: N_G(Q)]$ is a 2-power. Also, Q lies in a Hall $\{2, q\}$-subgroup

K of G. So, $Q \lhd K$ by Frobenius normal p-complement. This means $N_G(Q)$ contains a Sylow 2-subgroup of G; i.e., $Q \lhd G$.

THEOREM 1.F.2. *Let C be solvable and $\nu(S) = 0$ for every Sylow subgroup S of G. Then we have the following*: (1) $\gamma_R(G) = \nu(G)R$. (2) $\nu(G) =$ g.c.d.$(\{\nu(T) \mid T$ *a tight subgroup of* $G\})$. (3) $\nu(G)$ *is either* 0 *or* 1 *or* p *for some odd prime* p *dividing* $| G |$. (4) $\nu(G) = 0 \Leftrightarrow G$ *has no tight subgroups.*

Some immediate and useful consequences are:

COROLLARY 1.F.3. *Suppose G_1 and G_2 are both solvable groups, and* $(| G_1 |, | G_2 |) = 1$, *then* $\nu(G_1 \times G_2) = (\nu(G_1), \nu(G_2))$.

COROLLARY 1.F.4. *Let G be a group whose Sylow 2-subgroups are cyclic (possibly trivial). Then,* (i) $\nu(G) = 0$, 1, *or an odd prime dividing* $| G |$; (ii) $\nu(G) = 0 \Leftrightarrow G$ *has exactly one subgroup of prime order for each prime dividing* $| G |$.

COROLLARY 1.F.5. *Suppose G is a group whose order is not divibile by* 3, *then we have*: (i) $\nu(G)$ *is* 0, 1, *or some prime dividing* $| G |$; (ii) $\nu(G) = 0 \Leftrightarrow G$ *has exactly one subgroup of prime order for each prime dividing* $| G |$; (iii) *If* $\nu(G) = 2$, *then G has an elementary abelian subgroup of order* 4.

Prooof of Theorem 1.F.2. We break it into two cases: (i) when the Sylow 2-subgroup is cyclic, and (ii) when it is generalized quaternion.

Case (i). We assert in this situation, the following 3 conditions are equivalent: (a) G has exactly one subgroup of prime order for each prime dividing $| G |$; (b) $\nu(G) = 0$; (c) G has no tight subgroups. Indeed, (a) $\Rightarrow$ (b) by Theorem 1.A.4. (b) $\Rightarrow$ (c) is trivial. For (c) $\Rightarrow$ (a), we may assume $| G |$ is divisible by at least two primes. Let q be the largest prime divisor. Write $G = HQ$, Q a Sylow q-subgroup (hence, $Q \lhd G$ by 1.F.1). Since then $C_G(Q) \lhd G$, $C_G(Q)$ must contain every prime-order subgroup of G. Thus, either $C_G(Q) = G$, or else we are done by induction. But if $C_G(Q) = G$, then $G = H \times Q$ and we are again done by induction. This proves the assertion, and therefore also the subcase when G has no tight subgroups.

If G has tight subgroups with differing numerical invariant, then everything is clear. So, let us suppose G has at least one tight subgroup and any two have the same numerical invariant. Let q be the largest prime divisor of $| G |$, and Q a Sylow q-subgroup. Then, $Q \lhd G$, and $G = HQ$ where $q \nmid | H |$. If H has no tight subgroups, then H has a cyclic normal subgroup A such that A contains every prime-order subgroup of H. But then AQ contains every prime-order subgroup of G (and so also every tight subgroup of G). The

result follows by Proposition 1.E.3 and Theorem 1.D.2. So, assume H has a tight subgroup. Then, the centralizer $C_G(Q)$ must contain every prime-order subgroup of G. But, $C_G(Q) = Q \times C_H(Q)$. Hence, Theorem 1.D.3 says $\gamma_R(G) = \gamma_R(C_H(Q)) = \gamma_R(H) = \nu(H)R$. Therefore,

$$\nu(G) = \nu(H) = \text{g.c.d.}(\{\nu(T) \mid T \text{ is a tight subgroup of } G\}),$$

and Case (i) is done.

We remark here that the theorem is trivial if G has two tight subgroups with differing numerical invariant. Also, the theorem follows from the structural theorem of groups having no tight subgroups (see Appendix), if that is the case with G.

Case (ii). We suppose G is a minimal counter-example to the theorem. *Subcase* (1). G is *not* a $\{2, 3\}$-group. Let q be the largest prime dividing $|G|$, Q a Sylow q-subgroup. Then, Q is cyclic normal in G, and let Q_0 be the order-q subgroup of G. We have $C_G(Q_0) = Q \times L$, $q \nmid |L|$, so that $\gamma_R(C_G(Q_0)) = \gamma_R(L)$. If $C_G(Q_0)$ contains every prime-order subgroup of G, we get the result by induction. So, assume not. As $Q_0 \lhd G$, G has a tight subgroup T with $\nu(T) = q$. We then have by Theorem 1.D.4, $\gamma_R(G) = R \cap (\Gamma_R(H) + q \cdot RH)$, where $HQ = G$ and $q \nmid |H|$. We may clearly suppose H has no tight subgroups at all. In such case, there exists an element $\alpha \in \mathbf{Z}G$ with $\text{coeff}_\alpha(1) = 1$ and $\Gamma_{\mathbf{Z}}(G)\alpha = 0$. Let $x \in \mathbf{Z} \cap (\Gamma_{\mathbf{Z}}(H) + q \cdot \mathbf{Z}H)$. Write $x = c + qb$, $c \in \Gamma_{\mathbf{Z}}(H)$ and $b \in \mathbf{Z}H$. Then, $x\alpha = c\alpha + qb\alpha = qb\alpha \in q \cdot \mathbf{Z}H$, and $x = \text{coeff}_{x\alpha}(1)$. Thus, $\nu(G) = q = \text{g.c.d.}(\{\nu(W) \mid W \text{ a tight subgroup of } G\})$. The result follows. So, we must be in *Subcase* (2). G is a $\{2, 3\}$-group. Suppose G/G' (G' denotes commutator subgroup) is a 2-group. Then either G' contains every prime-order subgroup of G or G' is a Sylow 3-subgroup of G. We may suppose the latter, of course. But then, Proposition 1.E.7 gives the result. So, G/G' is not a 2-group. Take a subgroup M of G such that $G' \subseteq M$ and $[G: M] = 3$. We then have $M \lhd G$. Either M contains every prime-order subgroup of G (in which case we are done) or M is a Sylow 2-subgroup. In the latter situation, M is generalized quaternion. If $3 \mid |C_G(M)|$, then $G = M \times P$ with $|P| = 3$ and we are done. Otherwise, 3 divides $[N_G(M): C_G(M)]$, forcing $|M| = 8$, $|G| = 24$, and $G \cong SL(2, 3)$ which case we already know G satisfies the theorem. Contradiction.

Remark 1.F.6. The obvious question now is what if G is not solvable? Then Suzuki's theorem (see Appendix) applies. G has a subgroup G_0 such that $[G: G_0] \leqslant 2$, and $G_0 = H \times SL(2, p)$ for some prime $p \geqslant 5$, and moreover, $(|H|, |SL(2, p)|) = 1$, and every Sylow subgroup of H is cyclic. We have $\nu(G) = \nu(G_0)$. If p is *not* a Fermat prime (recall a Fermat prime is one of the form $2^{2^n} + 1$), then $\nu(G_0) = \text{g.c.d.}(\nu(H), p)$ and we know what

$\nu(H)$ is. In this case, we again obtain: $\nu(G) = \text{g.c.d.}(\{\nu(T) \mid T \text{ a tight subgroup of } G\})$. Suppose then p is a Fermat prime. If $\nu(H) = 0$, then $\nu(G) = \nu(SL(2,p))$, whatever that is—see also next section. If $\nu(H) = 1$, then obviously $\nu(G) = 1$. Suppose $\nu(H) = q$ for some prime q. By a result of Scharlau (see [7]), $q \mid \mid H \mid$ so that $q \nmid \mid SL(2,p) \mid$ and so q does not divide $\nu(SL(2,p))$. (We do know that $\nu(SL(2,p)) \equiv 0 \bmod p$, however.) Therefore, we are left to ask the following question:

QUESTION. *Is there an* $\alpha \in \mathbf{Z}(SL(2,5))$ *such that* $\text{coeff}_\alpha(1) = 1$, *and* $\Gamma_{\mathbf{Z}}(SL(2,5))\alpha = 0$?

A computer might be used to help resolve this issue. A "good" answer to this question would complete our investigation for the class of groups all of whose Sylow subgroups have their numerical invariant vanishing; in particular, $\nu(G_1 \times G_2)$ would be just the greatest common divisor of the $\nu(G_i)$, $i = 1, 2$ provided $(\mid G_1 \mid, \mid G_2 \mid) = 1$, extending our Corollary 1.F.3.

G. *General and Special Linear Groups.*

Let p be a prime, $n \geqslant F = GF(p^n)$, $G = SL(2,F)$, and $\tilde{G} = GL(2,F)$. Therefore, we have: $G \lhd \tilde{G}$, $\mid \tilde{G} \mid = GF(p^n + 1)\, p^n(p^n - 1)^2$, and $\mid G \mid = (p^n + 1)\, p^n(p^n - 1)$. Also, the centers are: $z(\tilde{G}) = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in F^*\}$, and $z(G) = G \cap z(\tilde{G}) = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}$. Let $P = \{\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \mid y \in F\}$. Since

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix},$$

we see there is an isomorphism between P and F^+. In particular, $\mid P \mid = p^n$, so that P is a Sylow p-subgroup of both G and $\tilde{G}$. Also, P is elementary abelian!

1.G.1. *By direct computations, one can obtain:* $N_G(P) = AP$, *where* $A = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) \mid a \in F^*\}$, *and* $C_G(P) = z(G)P$. *Notice* A *is naturally isomorphic to* F^*, *so that* A *is cyclic.*

Also, it is not difficult to see that G has a cyclic subgroup of order $p^n + 1$, and when p is an odd prime G has a unique involution.

PROPOSITION 1.G.2. *Let* p *be an odd prime.* (1) G *has no tight subgroups* $\Leftrightarrow n = 1$ *and* p *is a Fermat prime (i.e.,* p *is of the form* $2^{2^m} + 1$). (2) *If* $n > 1$ *or* p *is not a Fermat prime, then* G *has a tight subgroup* T *with* $\nu(T) = p$.

Proof. (1). Suppose G has no tight subgroups, and $n > 1$, then $\nu(P) = p$. So assume $n = 1$ and p not a Fermat prime. Choose $b \in F^*$ such that b has *odd* prime order q. Then, $q < p$, and $\langle \left(\begin{smallmatrix} b & 0 \\ 0 & b^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ is a nonabelian tight group of order qp. Contradiction again. Conversely, if $n = 1$ and p is a Fermat

prime, then using 1.G.1 above, it is easy to see that every odd order Sylow subgroup of G is cyclic. Also, G has a unique involution. So, G has no *abelian* tight subgroups, and also G has no dihedral tight subgroups. Suppose H is a tight subgroup of G. Then, $|H| = p_1 p_2$, p_1 and p_2 are primes with $p_1 < p_2$. As H is *not* dihedral, $p_1 > 2$. Also, p is the largest prime divisor of $|G|$ and $N_G(P)$ has no tight subgroups. Hence, $p > p_2$. So, $p_1 p_2 \mid p + 1$. Let H_2 be the Sylow p_2-subgroup of H. We have $H_2 \subseteq K$, where K is a *cyclic* group of order $p + 1$. Then, $\langle H, K\rangle \subseteq N_G(H_2)$. In particular, $p_1 \mid |C_G(H_2)|$, and yet $C_G(H_2)$ does not contain all order-p_1 subgroups of $N_G(H_2)$. This leads to a contradiction. (2) follows immediately from (1).

Remark 1.G.3. Suppose $p = 2$, then $\nu(SL(2, 2)) = 3$ as $SL(2, 2)$ is just S_3. When $n > 1$, then $SL(2, 2^n)$ contains both a copy of $SL(2, 2)$ and an elementary abelian Sylow 2-subgroup of order 2^n. Therefore, $\nu(SL(2, 2^n)) = 1$ whenever $n > 1$.

PROPOSITION 1.G.4. *For any odd prime p, and any $n \geqslant 1$, $\nu(SL(2, p^n) \equiv 0 \pmod{p}$.*

Proof. Let ϕ: $\mathbf{Z}G \to M_2(F)$ be the "evaluation" map (i.e., the obvious faithful degree-2 representation over $F = GF(p^n)$). We claim that $\Gamma_{\mathbf{Z}}(G)$ is contained in $\mathrm{Ker}(\phi)$. This would then give $\nu(G)\mathbf{Z} \subseteq \mathbf{Z} \cap \mathrm{Ker}(\phi) = p\mathbf{Z}$. Now then, let H be a subgroup of G with prime order q, and $H = \langle h\rangle$. $\phi(\sigma_{\mathbf{Z}}(H)) = f(\phi(h))$, where $f(X) = \sum_{i=0}^{q-1} X^i \in F[X]$. Let g be the minimal polynomial for $\phi(h)$ over F. Then, $g(X)$ divides the characteristic polynomial for $\phi(h)$, which is

$$X^2 - \mathrm{Tr}(\phi(h))X + \mathrm{Det}(\phi(h)) = X^2 - \mathrm{Tr}(\phi(h))X + 1.$$

Also, $g(X)$ divides $X^q - 1 = (X - 1)f(X)$, and $g(X) \neq X - 1$. Therefore, $g(X) \mid f(X)$ or $g(X) = (X - 1)^2$. Suppose the latter, then $\phi(h)$ is similar to a matrix $\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$ for some nonzero c in F. But, this then gives: $q = p$ and

$$f(\phi(h)) \sim f\left(\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}^i = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & ic \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} p & cp(p-1)/2 \\ 0 & p \end{pmatrix} = 0,$$

so that $f(\phi(h)) = 0$ and $g(X) \mid f(X)$. Hence, $f(\phi(h)) = 0$ and $\sigma_{\mathbf{Z}}(H)$ belongs to $\mathrm{Ker}(\phi)$. We are finished.

COROLLARY 1.G.5. *Suppose p is an odd prime. If either $n > 1$ or p is not a Fermat prime, then $\nu(SL(2, p^n)) = p$.*

COROLLARY 1.G.6. *Suppose p is an odd prime, and R a field with characteristic p. Then, $\gamma_R(SL(2, p^n)) = 0$, for all $n \geqslant 1$.*

Proof. Replace $\mathbf{Z}$ with R and replace F with an algebraic closure of FR in the above argument.

PROPOSITION 1.G.7.

$$\nu(GL(2, p^n)) = \begin{cases} 3 & \text{if } p = 2 \text{ and } n = 1 \\ 1 & \text{otherwise.} \end{cases}$$

Proof. If $n = 1$, then $GL(2, p^n) = SL(2, p^n) = S_3$, when $p = 2$. If $p = 2$ and $n > 1$, then $\nu(SL(2, p^n)) = 1$ by Remark 1.G.3, so that $GL(2, p^n)$ would have the same numerical invariant. When p is odd, the subgroup $\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle$ is elementary abelian of order 4, and $\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ is non abelian tight of order $2p$.

COROLLARY 1.G.8. *If $m > 2$, then $\nu(SL(m, p^n)) = 1$.*

Proof. For $p = 2$, $SL(m, p^n)$ contains a copy of $SL(3, 2)$, which is a nonabelian simple group. For p odd, the map $GL(m - 1, p^n) \to SL(m, p^n)$ given by

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & \mathrm{Det}(A)^{-1} \end{pmatrix}$$

is a monomorphism, and $\nu(GL(m - 1, p^n)) = 1$.

PROPOSITION 1.G.9. *$\gamma_R(SL(2, 3)) = 0$. For a Fermat prime p, $\nu(SL(2, p)) = 0$ if and only if $p = 3, 5$. Thus, when $p > 5$, Proposition 1.G.4 gives*

$$\nu(SL(2, p)) = pt$$

for some $t \neq 0$.

Proof. See Appendix.

2. SOME APPLICATIONS OF THE NUMERICAL INVARIANT

In this short Section we sketch some applications of the numerical invariant $\nu(G)$ to the study of the behaviour of certain arithmetical invariants of quadratic forms and algebraic number theory under a finite Galois extension with Galois group G. The arithmetic entities considered here are: height, number of square classes, generalized Kaplansky's u-invariant, size of the Witt ring, and class number of a number field. A connection of $\nu(G)$ with group representations is also cited.

A. *Applications to Quadratic Forms*

Let S/R be a finite Galois ring extension with Galois group G. There is the obvious homomorphism $f: \oplus_L W_i(L) \to W_i(S)$ of torsion subgroups of the Witt groups—here the direct sum is taken over all fixed subrings $L = S^H$, H a subgroup of G of prime order. As in [3], the cokernel of f is annihilated by the numerical invariant $v(G)$. Therefore, we have: *Let h^0 be the least common multiple of the heights $h(L)$'s. If $1 = (h^0, v(G))$, then f is surjective. In particular, $h(S) \leqslant h^0$. Moreover, if R is semilocal, then f is surjective whenever $v(G)$ is odd.*

Recall that the generalized Kaplansky's u-invariant is the largest anisotropic dimension of torsional spaces. (For general rings one may restrict nonsingular spaces defined over projective modules of constant rank.) Whenever the map f above is surjective, we have: $u(S) \leqslant n(G) \cdot \mathrm{Max}_L\, u(L)$, where $n(G)$ is the number of subgroups of G of prime order. Clearly,

$$n(G) < \sum_{p \mid |G|} \binom{|G|}{p} < 2^{|G|}.$$

There are known results on $n(G)$, see [10].

Pfister had communicated (unpublished) to us the following beautiful result of his [5]:

THEOREM (Pfister). *If S/R is a field extension of degree n, then $h(S) \leqslant 2nh(R)$*[1].

This, of course, greatly improves the original estimates given in [3]. We illustrate below how the knowledge of the numerical invariant, when combined with Pfister's theorem, can further sharply improve the estimate for the height behavior. Two typical cases are: (1) Suppose G is a finite solvable group, and H is a minimal normal subgroup of G. It is well-known that H is elementary abelian. Let $L = S^H$ be the fixed subfield. If $|H| = p^t$ is odd, then $h(S) \leqslant 2p \cdot h(L)$. Otherwise, $h(S) \leqslant 2p^t \cdot h(L)$. Continuing, we obtain a normal series $G \rhd H_1 \rhd \cdots \rhd H_m \rhd 1$ where H_j is a minimal normal subgroup of G containing H_{j+1}. Thus, the factor groups H_j/H_{j+1} are all elementary abelian of order $p_j^{e_j}$. (The primes p_j's are not necessarily distinct.) Thus, $h(S) \leqslant 2^{m+1}(\prod_{p_j \text{ odd}} p_j)(\prod_{p_j=2} p_j^{e_j}) \cdot h(R)$. At worst, for all odd p_j's the factor groups H_j/H_{j+1} are all cyclic (e.g., when G is abelian) in which case we recover Pfister's estimate. Now, we treat the abelian case. (2) Here the numerical invariant vanishes if and only if G is cyclic. Let S_p be a Sylow p-subgroup of G which is not cyclic, T_p its maximal elementary abelian subgroup. For p odd, $h(S) \leqslant 2p \cdot h(A_p)$, where A_p is the fixed field of T_p.

[1] Actually, a stronger result was proved by Pfister. Namely, if $m(X)$ denotes the *reduced-height* of X (i.e., $m(X)$ is the minimal positive integer such that every sum of squares in X is already a sum of $m(X)$ squares), Pfister proved: $m(S) \leqslant n \cdot m(R)$.

Now, consider S_p/T_p and continue this descent until we get a cyclic group at which stage one applies the Pfister estimate. Similarly for the other odd primes dividing $|G|$. Thus, the estimate here can be efficiently achieved from the elementary divisors of the Sylow subgroups of G.

Still let S/R be a Galois field extension with group G. If R^*/R^{*2} is finite and its cardinality q_R, is q_S also finite? When G is a 2-group, the answer is yes (see [2], [4]). In general, if the extension is not Galois—even if still a 2-power degree—Lam showed [4] the answer is no. For any odd extension, a theorem of Springer says $q_S \geqslant q_R$. Suppose now G is odd (so solvable) and $\nu(G) \neq 0$. So, $\nu(G)$ is either 1 or an (odd) prime dividing $|G|$. If $c \in S^*$, H a subgroup of G of prime order, we have: $\sigma(H) \cdot c = \prod_{h \in H} h(c) = \mathrm{Norm}_{S/L}(c)$, where L is the fixed field of H. So, the map $f: \prod_L L^*/L^{*2} \to S^*/S^{*2}$ is surjective. Thus, $q_S \leqslant \prod_L q_L$, and the finiteness of q_S depends upon these q_L's (L ranging over all subfield of prime index in S). [This much carries over for rings as well.] Now, the Witt ring of a field F is finite if and only if F is formally nonreal with q_F finite. In that case, we have: $u(F)\, q_F \leqslant |W(F)| \leqslant 2^{q_F}$ (see [4]). Hence, a discussion for the estimate of the size of $W(S)$ can be made.

If S/R is an extension corresponding to the rings of integers in a finite extension of number fields E/F, then S/R is Galois if and only if E/F is unramified. A similar argument shows that every S-space (i.e., unimodular S-lattice) is similar to an orthogonal sum of L-spaces ($L = S^H$ where H is a subgroup of prime order). This fact may be useful in the genus theory of integral quadratic forms.

B. *Application to Class Number Relations*

Similar to the treatment in Section 2.A for the behavior of square classes, we can apply to the ideal class group of a global field. Ideal class groups for more general rings may be analogously studied.] Let E/F be a finite Galois extension of global fields with Galois group G. As before, we have $f: \prod_K C(K) \to C(E)$ be the class groups. G acts on $C(E)$ in the usual fashion. For any fractional ideal A in E, and H a subgroup in G of prime order, the ideal class in E represented by $\sigma(H) \cdot A = \prod_{h \in H} h(A)$ is just the image under f of the ideal class in L represented by $\mathrm{Norm}_{E/L}(A)$, where L is the fixed field of H. So, again $\nu(G)$ annihilates $\mathrm{Coker}(f)$ and the full force of Section 1 can be brought to bear to relate the class number $c(E)$ of E in terms of the class numbers $c(K)$. In particular, when $\nu(G) = 1$, f is surjective and $c(E)$ divides the least common multiple of the $c(K)$'s. When concentrating on a given p-part of $c(E)$, one observes that if $\nu(G)$ is relatively prime to p then the Sylow p-subgroups of $C(E)$ lie in the image of f.

Instead of studying the ideal class groups, one can surely deal with other arithmetical entities as well; e.g., groups of units, rings of integers, and so forth.

C. *Connection with Group Representations*

A representation ρ of a group G is fixed-point-free if the linear transformation $\rho(g)$ does not have 1 for its eigen-value for all $g \neq 1$. Scharlau [7] showed the link between fixed-point-free representation with the vanishing of the numerical invariant. This means, in particular, for solvable groups G, G has a fixed-point-free representation if and only if G does not possess any tight subgroups, by Theorem 1.F.2(4). [For nonsolvable groups, the nonexistence of tight subgroups (e.g., $SL(2, 17)$ see Proposition 1.G.2) does not assure the vanishing of $\nu(G)$.] Thus, the question arises as to how do we characterize finite solvable groups having no tight subgroups? We state the result here and refer the reader to the Appendix for greater details.

PROPOSITION, *Let G be a finite solvable group. Then G has no tight subgroups if and only if G satisfies one of the following*: (i) *G has exactly one subgroup of prime order for each prime dividing $|G|$*, (ii) *G has a generalized quaternion Sylow 2-subgroup and also G has a subgroup G_0 such that $[G: G_0] \leqslant 2$ and $G_0 = H \times SL(2, 3)$, where $(|H|, 6) = 1$ and H has exactly one subgroup of prime order for each prime dividing $|H|$.*

APPENDIX

A. We wish to show here that $\gamma_R(SL(2, 3)) = 0$. It is not difficult to see that a group G of order 24 is isomorphic to $SL(2, 3)$ if and only if one of the following equivalent statements holds: (i) G has no subgroup of order 12: (ii) G has a quaternion Sylow 2-subgroup and has no normal Sylow 3-subgroup; (iii) G has a unique involution and has no normal Sylow 3-subgroup. It follows that G has no tight subgroups and G is generated by its Sylow 3-subgroups. In terms of generators and relations we have: let $G = SL(2, 3)$ with Sylow 2-subgroup Q, then there exist elements a, b, c, d in G such that $Q = \langle a, b\rangle$, $D = \langle d\rangle \in \mathrm{Syl}_3(G)$, $A = \{1, a^2\}$ = center of G, and $a^d = d^{-1}ad = b$, $b^d = c = ab$. Denote by $ccl(g)$ the conjugacy class of g, we have:

$$
\begin{aligned}
x_7 &= a + b + c + a^{-1} + d^{-1} + c^{-1} && = \sum ccl(a)\\
x_6 &= a^2d^2 + ad^2 + bd^2 + cd^2 && = \sum ccl(a^2d^{-1}),\\
x_5 &= a^2d + a^{-1}d + b^{-1}d + c^{-1}d && = \sum ccl(a^2d),\\
x_4 &= d^{-1} + a^{-1}d^{-1} + b^{-1}d^{-1} + c^{-1}d^{-1} && = \sum ccl(d^{-1}),\\
x_3 &= d + ad + bd + cd && = \sum ccl(d),\\
x_2 &= a^2 && = \sum ccl(a^2),\\
x_1 &= 1 && = \sum ccl(1).
\end{aligned}
$$

Then, $\{x_1, \ldots, x_7\}$ is a $\mathbf{Q}$-basis for the center $z(\mathbf{Q}G)$ of the rational group algebra $\mathbf{Q}G$, and also $z(\mathbf{Z}G) = \sum \mathbf{Z}x_i$. It is easy to see that the numerical

invariant $\nu(G) = 0$ if and only if $\gamma_{\mathbf{Q}}(G) = 0$. From the proof of Satz 1 in [7], one sees that for any field F of characteristic zero, the following three statements are equivalent: (i) $\gamma_F(G) = 0$; (ii) there exists an $\alpha \in z(FG)$ such that $\Gamma_F(G) \cdot \alpha = 0$; (iii) G has a fixed-point-free representation over F. This element we shall find below, so that we can deduce $\nu(G) = 0$. Moreover, if we can find a central annihilator $\alpha \in (\mathbf{Z}G)$ with $\alpha \cdot \Gamma_{\mathbf{Z}}(G) = 0$ and also $\text{coeff}_\alpha(g_0) = 1$ for some $g_0 \in G$, then we would surely have $\gamma_R(G) = 0$ for all R. In order to annihilate $\Gamma_{\mathbf{Z}}(G)$, it is sufficient to have an element in the center of $\mathbf{Z}G$ that annihilates both $\sigma(A)$ and $\sigma(D)$. Taking

$$\alpha = (1 - a^2)(-2x_1 + x_3 + x_4),$$

one sees that α lies in $z(\mathbf{Z}G)$, and $\sigma(A) \cdot \alpha = 0 = \sigma(D) \cdot \alpha$. Also, $\text{coeff}_\alpha(d^{-1}) = 1$. We are done.

B. *On Groups Having no Tight Subgroups*

Recall a finite group G satisfies condition $(*)$ if G has exactly one prime-order subgroup for each prime dividing $|G|$. This means, therefore, all the odd-order Sylow subgroups of G are cyclic and the Sylow 2-subgroups (if there are any) are either cyclic or generalized quaternion. A tight group of order pq $(p < q)$ is given by generators and relations as follows:

$$\langle a, b \mid a^p = b^q = 1,\ a^{-1}ba = b^r \rangle$$

and we know that $r^p \equiv 1 \pmod{q}$, and $p \mid q - 1$. If we "loosen-up" this group by considering the group $G = \langle a, b \mid a^{p^2} = b^q = 1,\ a^{-1}ba = b^r \rangle$, then we see a^p commutes with b and so lies in the center of G. This group G satisfies condition $(*)$ and is not nilpotent. The following result characterizes all finite groups having no tight subgroups:

THEOREM. *A finite group G does not have any tight subgroups if and only if G satisfies one of the following two conditions*: (i) *G satisfies condition* $(*)$; (ii) *a Sylow 2-subgroup of G is generalized quaternion and G has a subgroup G_0 such that $[G: G_0] \leqslant 2$ and $G_0 = H \times SL(2, p)$ where H satisfies condition* $(*)$, *p is a Fermat prime (i.e., of the type $p = 2^{2^n} + 1$), and $(|H|, |SL(2, p)|) = 1$.*

Proof. Suppose G is not solvable. Suppose also G has no tight subgroups. [Since groups satisfying condition $(*)$ are solvable, G must necessarily be in the case (ii).] A deep theorem of Suzuki's (see [8]) then says G has a generalized quaternion Sylow 2-subgroup, and has a subgroup G_0 of index $[G: G_0] \leqslant 2$ where $G_0 = H \times SL(2, p)$ with p an odd prime and H has all its Sylow subgroups cyclic, and finally $(|H|, |SL(2, p)|) = 1$. Since the order of H is odd (and so solvable) and has no tight subgroups, H satisfies condition $(*)$—see the solvable part of the proof below. Also, $SL(2, p)$ has no tight subgroups either, p must be a Fermat prime by Proposition 1.G.2(1).

Conversely, suppose G is in the case (i), then surely G has no tight subgroups (see Theorem 1.A.4). And when G is in the case (ii), G_0 contains every prime-order subgroup of G and hence also contains every tight subgroup of G. But, G_0 has no tight subgroups.

It remains to show the only-if part when G is solvable. Suzuki remarked in [8] that his classification theorem in the solvable situation had been done by Zassenhaus in [11]. The version given by Zassenhaus we found inconvenient for our purposes, as we prefer to deal with condition $(*)$ in which case the vanishing of the invariant ideal is given by our Theorem 1.A.4 at the very outset. Thus, we choose to characterize these groups in the form given above, and this is our justification to include its proof in the Appendix here.

So now G is finite solvable and does not satisfy condition $(*)$. Since G has no tight subgroups, G has cyclic odd-order Sylow subgroups and has at most one involution. Choose $Q \in \mathrm{Syl}_2(G)$ and so Q must be generalized quaternion. [If Q were cyclic, then G having no tight subgroups is equivalent to having G satisfy condition $(*)$.] Suppose $3 \nmid |G|$. By Frobenius' normal p-complement, $G = QN$, where $N \lhd G$. Let y be the involution of Q. Then, $\langle y \rangle N$ contains every prime-order subgroup of G. But then $\langle y \rangle N$ satisfies condition $(*)$ so that G satisfies condition $(*)$. A contradiction. Thus, $|G|$ is divisible by 3. Let H_0 be a Hall $\{2, 3\}'$-subgroup of G. Since H_0 lies inside a Hall $3'$-subgroup of G, H_0 is normalized by a Sylow 2-subgroup of G. Thus, $[G: N_G(H_0)]$ is a 3-power. But, H_0 lies inside a Hall $2'$-subgroup of G as well, and H_0 is normal in any such Hall subgroup, by Burnside's normal p-complement theorem. Hence, $N_G(H_0)$ contains a Sylow 3-subgroup of G. So, $H_0 \lhd G$ and H_0 is the unique Hall $\{2, 3\}'$-subgroup of G. As H_0 has no tight subgroups of G, H_0 satisfies condition $(*)$. Thus, if p is a prime divisor of $|G|$ and $p > 3$, then G has exactly one subgroup of order p. Also, G has exactly one subgroup of order 2. This implies, since G does not satisfy condition $(*)$, G must have more than one element of order 3.

Suppose P_0 is an order-3 subgroup of G. Then there is a Hall $2'$-subgroup K of G such that P_0 is contained in K. We have $K = PH_0$, with $P \in \mathrm{Syl}_3(G)$. But, K had odd order and also no tight subgroups, so that K satisfies condition $(*)$. So, P_0 is the only order-3 subgroup of K. On the other hand, $[K: C_K(P_0)]$ divides $|\mathrm{Aut}(P_0)| = 2$. This means P_0 is contained in the center of K and H_0 contained in $C_G(P_0)$. Therefore, H_0 is the largest normal $\{2, 3\}'$-subgroup in G and centralizes *every* order-3 element of G.

Let S be a Hall $\{2, 3\}$-subgroup of G. If $S = G$, then we shall be done by the Proposition given below in this section. So, suppose S is a proper subgroup. By induction, S satisfies condition $(*)$ or $|S| \in \{24, 48\}$ with $SL(2, 3) \subseteq S$. Suppose S satisfies condition $(*)$. Then, S has exactly one subgroup of order 3. We have $G = SH_0$, and S has a unique subgroup S_0

of order 6. Thus, S_0H_0 is a subgroup of G containing every prime-order subgroup of G. But, $S_0H_0 = S_0 \times H_0$ and S_0 is cyclic. So, S_0H_0 (hence, also G) satisfies condition $(*)$. Again, a contradiction. When S does not satisfy condition $(*)$, there is a subgroup S_0 of S with $[S: S_0] \leqslant 2$ and $S_0 \cong SL(2, 3)$. We have then $[G: S_0H_0] \leqslant 2$. Since S_0 is generated by its order-3 elements and since H_0 centralizes every order-3 elements of G, we have $S_0H_0 = S_0 \times H_0$. The proof is completed.

We now prove the Proposition that was used in the above proof.

PROPOSITION. *Let G be a $\{2, 3\}$-group and a Sylow 2-subgroup of G is generalized quaternion. If G has no tight subgroups, then either G satisfies condition $(*)$ or G has a subgroup G_0 such that $[G: G_0] \leqslant 2$ and $G_0 \cong SL(2, 3)$.*

Proof. Since G has no tight subgroups, G has exactly one involution. Choose $T \in \mathrm{Syl}_2(G)$ and $P \in \mathrm{Syl}_3(G)$. We know that P is cyclic. In particular, the order-3 subgroups of G are all conjugates in G. Assume G does not satify condition $(*)$. Then G has no nontrivial normal 3-subgroup.

Case 1. $T \lhd G$. $C_G(T)\ T = T \times P_0$ where P_0 is some cyclic 3-subgroup of G. But, P_0, being also a normal 3-subgroup in G, is trivial. Thus, $C_G(T) = z(T)$. But, $9 \nmid [G: C_G(T)]$ and $3 \mid [G: z(T)]$. Hence, $|\ G\ | = 24$ and $G \cong SL(2, 3)$—see Section 3.A.

Case 2. $T \trianglelefteq G$ and $3 \mid [G: G']$ (G' is the commutator of G). Let M be a subgroup of G with $G' \subseteq M$ and $[G': M] = 3$. We have $M \lhd G$. Either 9 does not divide $|\ G\ |$ or M contains every prime-order subgroup of G. Suppose the former. Then G' is a 2-group and $G' \subseteq T$, forcing $T \lhd G$. A contradiction. So, $9 \mid |\ G\ |$ and M contains every prime-order subgroup of G. If M satisfies condition $(*)$, then so does G, contrary to assumption. But M has no tight subgroups. Hence, by induction M has a subgroup H such that $[M: H] \leqslant 2$ and $H \cong SL(2, 3)$. Let $T_0 = H \cap T$. Then $T_0 \in \mathrm{Syl}_2(H)$. T_0 is a largest normal 2-subgroup in H, so $T_0 \lhd M$. But, $[T: T_0] \leqslant 2$ so that either T_0 is the largest normal 2-subgroup in M or else T itself is the largest normal 2-subgroup of M. By case 1 (applied to M) the second possibility cannot occur. Therefore, $T_0 \lhd G$. We also have $|\ P\ | = 9$. Since T_0 is generalized quaternion, T_0 is centralized by every order-3 subgroup of G. Contradiction!

Case 3. $T \trianglelefteq G$ and G/G' is a 2-group. Choose a subgroup M of G with $G' \subseteq M$ and $[G: M] = 2$. Then, $M \lhd G$ and M contains every prime-order subgroup of G. Also, M has no tight subgroups and M does not satisfy condition $(*)$. [Note that if M satisfies condition (*), then G does too.] Thus, M has a subgroup H such that $[M: H] \leqslant 2$ and $H \cong SL(2, 3)$. If $M = H$ we are finished. So, let $[M: H] = 2$. Take $T_0 \in \mathrm{Syl}_2(H)$. Then, $T_0 \lhd M$. By case 1, M cannot have a normal Sylow 2-subgroup so that $T_0 \lhd G$. In partic-

ular, $9 \nmid |G|$ [since otherwise every order-3 element of G lies in $C_G(T_0)$]. Let $n_3(G) = |\mathrm{Syl}_3(G)|$. Then, we have $n_3(G) = n_3(M) = n_3(H) = 4$. Let $K = \mathrm{Core}_G(N_G(P))$ where $P \in \mathrm{Syl}_3(H)$. Then G/K is isomorphic to a subgroup of S_4 and $|G| = 4 \cdot |H| = 4 \cdot 24$. Also, $3 \nmid |K|$, so K is a 2-group. We have $|K| \geqslant 4$ and $|K \cap T_0| = 2$. Consider T_0K. We have $T_0K \lhd G$ and $|T_0K| \geqslant 4 \cdot |K| \geqslant 16$. But, T_0K is generalized quaternion. Contradiction again. Proof is finished.

C. Suppose G is of the case (ii) in the above theorem. Then, $\nu(G) = \nu(G_0) = \nu(A \times SL(2, p)) = \nu(SL(2, p))$, where A is the subgroup of H generated by its prime-order subgroups. It is also interesting to observe that in the nonsolvable cases, the lowest Fermat prime ($p = 5$) is the only one that gives a vanishing numerical invariant. This is because from the character table for $SL(2, p)$ one can see that $SL(2, 5)$ has a fixed-point-free representation while the higher Fermat primes don't. On the other hand. Proposition 1.G.4 says for any odd prime $\nu(SL(2, p) \equiv 0 \pmod{p}$. Thus, we have: *Let p be a Fermat prime. $\nu(SL(2, p) = 0$ if and only if $p = 3, 5$. Moreover, when $p > 5$, p divides $\nu(SL(2, p))$.*

Acknowledgment

We would like to express our hearty thanks to S. K. Wong for several useful and stimulating conversations as well as for the use of some of his private (Japanese) character tables.

Note added in proof. The question raised on page 589 has been answered affirmatively with the aid of a computer. In particular, therefore, $\nu(G_1 \times G_2) = \text{g.c.d.}(\nu(G_1), \nu(G_2))$ for any two finite groups G_1 and G_2 having relatively prime orders. This extends Corollary 1.F.3. For details, see the forthcoming paper, "An invariant ideal of a group ring of a finite group. II," to appear in *Proc. Amer. Math. Soc.*

References

1. D. Gorenstein, "Finite Groups," Harper and Row, New York, 1968.
2. H. Gross and H. Fischer, Non real fields k and infinite dimensional k-vector spaces, *Math. Ann.* **159** (1965), 285–308.
3. M. Knebusch and W. Scharlau, Über das Verhalten der Witt-Gruppe bei galoischen Körpererweiterungen, *Math. Ann.* **193** (1971), 189–196.
4. T. Y. Lam, "The Algebraic Theory of Quadratic Forms," Benjamin, New York, 1973.
5. A. Pfister, private communication.
6. W. Scharlau, Induction theorems and the structure of the Witt group, *Invent. Math.* **11** (1970), 37–44.
7. W. Scharlau, Eine Invariante endlicher Gruppen, *Math. Z.* **130** (1973), 291–296.

8. M. SUZUKI, On finite groups with cyclic Sylow subgroups for all odd primes, *Amer. J. Math.* **77** (1955), 657–691.
9. M. SUZUKI, Finite groups in which the centralizer of any element of order 2 is 2-closed, *Ann. Math.* **82** (1965), 191–212.
10. H. ZASSENHAUS, "The Theory of Groups," Chelsea Publishing Co., New York, 1958.
11. H. ZASSENHAUS, Über endliche Fastkörper, *Abh. Math. Sem. Univ. Hamburg* 11 (1936), 187–220.